



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/517,884	03/03/2000	George Fleming	US008002	5479

7590 04/05/2004
U S Philips Corporation
Corporate Patent Counsel
580 White Plains Rd
Tarrytown, NY 10591

EXAMINER

ZIA, MOSSADEQ

ART UNIT PAPER NUMBER

2134

DATE MAILED: 04/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/517,884

Applicant(s)

FLEMING ET AL.

Examiner

Mossadeq Zia

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-17 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on ____ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. ____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|--|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date ____ | 6) <input type="checkbox"/> Other: ____ |

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1, 2, 3, 5, 7, 12 are rejected under 35 U.S.C. 102(b) as anticipated by U.S. Patent No. 5,148,481, Abraham et al.

3. Regarding claim 1, Abraham et al discloses a processing system comprising:
an application device (processor, Abraham, fig. 3, label 51, col. 6, line 35) that is configured to communicate information with a physical-layer access device via a link-layer (RS-232, Abraham, fig. 3, label 61) access device,
a node controller (cryptographic adapter) that is configured to control the link-layer access device (Abraham, fig. 1, label 29, 30, col. 3, line 50-52),
the link-layer access device (workstation, Abraham, fig. 3, label 25), operably coupled to the application device (processor), the node controller (cryptographic adapter), and the physical-layer access device, that is configured to facilitate an exchange of the information from and to the application device with data that is communicated to and from the physical-layer access device (Abraham, fig. 3, label 25, 53, col. 6 line 36-40);

wherein, the link-layer access device is further configured to provide, in response to one or more commands from the node controller (Abraham, fig. 12, col. 12, line 66-67), one or more cryptographic items based on one or more parameters from the node controller (Abraham, col. 8, line 14-18).

4. Regarding claim 2 and 3, Abraham et al discloses the processing system of claim 1, wherein the one or more cryptographic items include at least one of:

a digital signature (MAC, Abraham, col. 7, line 40),

a verification of a digital signature (MAC verification, Abraham, col. 7, line 39-40), and

a cryptographic key item (Abraham, col. 6, line 65-68).

5. Regarding claim 5, Abraham et al discloses the processing system of claim 1, wherein the node controller (cryptographic adapter) is configured to effect an “exchange of a cryptographic key” (session key) with an other processing system, and the one or more cryptographic items from the link-layer access device includes the cryptographic key (Abraham, col. 14, line 15-20, fig. 14, label 329).

6. Regarding claim 7, Abraham et al discloses a link-layer access device comprising:

an application-layer interface device processor (Abraham, fig. 3, label 51, col. 6, line 35), that is configured to communicate information with an application-layer device (RS-232, Abraham, fig. 3, label 61),

a physical-layer interface device that is configured to communicate data with a physical layer device (Abraham, fig. 1, label 29, 30, col. 3, line 50-52),

a buffer device (workstation, Abraham, fig. 3, label 25), operably coupled to the application-layer interface device and the physical-layer interface device, that is configured to

Art Unit: 2134

facilitate an exchange of the information of the application-layer device and the data of the physical-layer device (Abraham, fig. 3, label 25, 53, col. 6 line 36-40),

a controller interface device (Abraham, fig. 4, label 97), operably coupled to the application-layer interface device (processor) and the physical-layer interface device (cryptographic adapter), that is configured to facilitate control of the exchange of information and data, and (Abraham, col. 6, line 37-40)

an accelerator (encryption processor, Abraham, fig. 4, label 85), operably coupled to a controller via the controller interface device (Abraham, fig. 1, label 29), that is configured to compute one or more cryptographic items, in response to one or more cryptographic commands from the controller (Abraham, fig. 12, col. 12, line 66-67), and to thereafter communicate the one or more cryptographic items to the controller (Abraham, col. 7, line 35-38, col. 8, line 14-18).

7. Regarding claim 12, see reasoning in claim 1 and 7 above.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 4, 6, 8, 11, 15, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,148,481, Abraham et al as applied to claims 1, 7, 12 above, and further in

Art Unit: 2134

view of "Design and Implementation of Arithmetic Processor F_2^{155} for Elliptic Curve Cryptosystems" by Sutikno et al.

10. Regarding claim 4, 8, and 15, Abraham et al discloses the processing system of claim 1, but fail to show that it includes a multiplication device that is configured to derive a second point on an elliptic curve from a first point on the elliptic curve, based on the one or more of the parameters from the node controller.

Sutikno teaches how to design and implement an arithmetic processor (coprocessor) with an efficient architecture and apply it to the Elliptical Curve Cryptosystem or ECC (Sutikno, col. 1, line 10-14, and 40-41 through col. 2 line 1-2). Sutikno further teaches that the coprocessor (multiplication device) has good flexibility which can perform arithmetic operation for computation in ECC applications (Sutikno, col. 8, line 5-8) such as ElGamal ECC, ECDSA, and others. Sutikno also teaches deriving a second point from the first point on the elliptic curve is a function in ECC (Sutikno, col. 2, line 18, specifically the equation) from inputs (one or more of the parameters) (Sutikno, col. 5, lines 30-33) and where the Main Controller controls all the process to the of the arithmetic processor (Sutikno, col. 7, line 7-9).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Abraham as per teaching of Sutikno to include the benefits of having a ECC coprocessor in the node controller because of the small area and the flexibility of the arithmetic processor making it suitable for IC card applications (Sutikno, col. 8, line 8-10).

11. Regarding claim 6, 11, and 17, Abraham et al discloses the processing system of claim 1 however fail to show that the commands from the node controller include:

a basepoint multiply command,

a point multiply command,
an EC-DNA verify command, and
an EC-DNA sign command.

In regards to multiply commands and EC-DNA commands, Sutikno teaches how to design and implement an arithmetic processor (coprocessor) with an efficient architecture and apply it to the Elliptical Curve Cryptosystem or ECC (Sutikno, col. 1, line 10-14, and 40-41 through col. 2 line 1-2). Sutikno further teaches that the coprocessor (multiplication device) has good flexibility which can perform arithmetic operation for computation in ECC applications (Sutikno, col. 8, line 5-8) such as ElGamal ECC, ECDSA, and others.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Abraham as per teaching of Sutikno to include the benefits of having a ECC coprocessor in the node controller because of the small area and the flexibility of the arithmetic processor making it suitable for IC card applications (Sutikno, col. 8, line 8-10).

Response to Arguments

12. Applicant's arguments filed page 2-3 have been fully considered but they are not persuasive.

13. Applicant's arguments, see 3rd paragraph from bottom, filed on page 2 of 3, with respect to contradictorily identifies the IC reader as the link layer access device. The identifications have been readdressed and addressed the issue Applicant raises. See newly revised action above with Abraham where IC reader is no longer identified.

Art Unit: 2134

14. Applicant's arguments, see 2nd paragraph from bottom, filed on page 2 of 3, with respect to Abraham's item 61 & 67 both corresponding to Applicants link level access device where item 61 & 67 are no longer identified. The issue has been addressed by the newly revised action above with Abraham.

15. Applicant's arguments, see last paragraph, filed on page 2 of 3, with respect the node controller that controls Abraham's link level access device. The issue has been addressed by the newly revised action above with Abraham.

Remarks

16. Applicant states there are 1-16 claims pending. This is stated on 1st line on page 2 of 3 and it is incorrect. There are 1-17 claims filed by the applicant.

17. Claims not addressed directly in this Office action will refer to rejections in the previous Office action, thusly claims 1-17 are not allowed.

Conclusion

18. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after

Art Unit: 2134

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

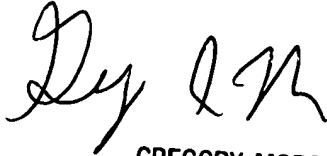
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mossadeq Zia
Examiner
Art Unit 2134

mz
3/31/04


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100